09941508 SHEET
BLON ET AL (703) 413-3000
DOCKET #_____SHEET 1 OF 26

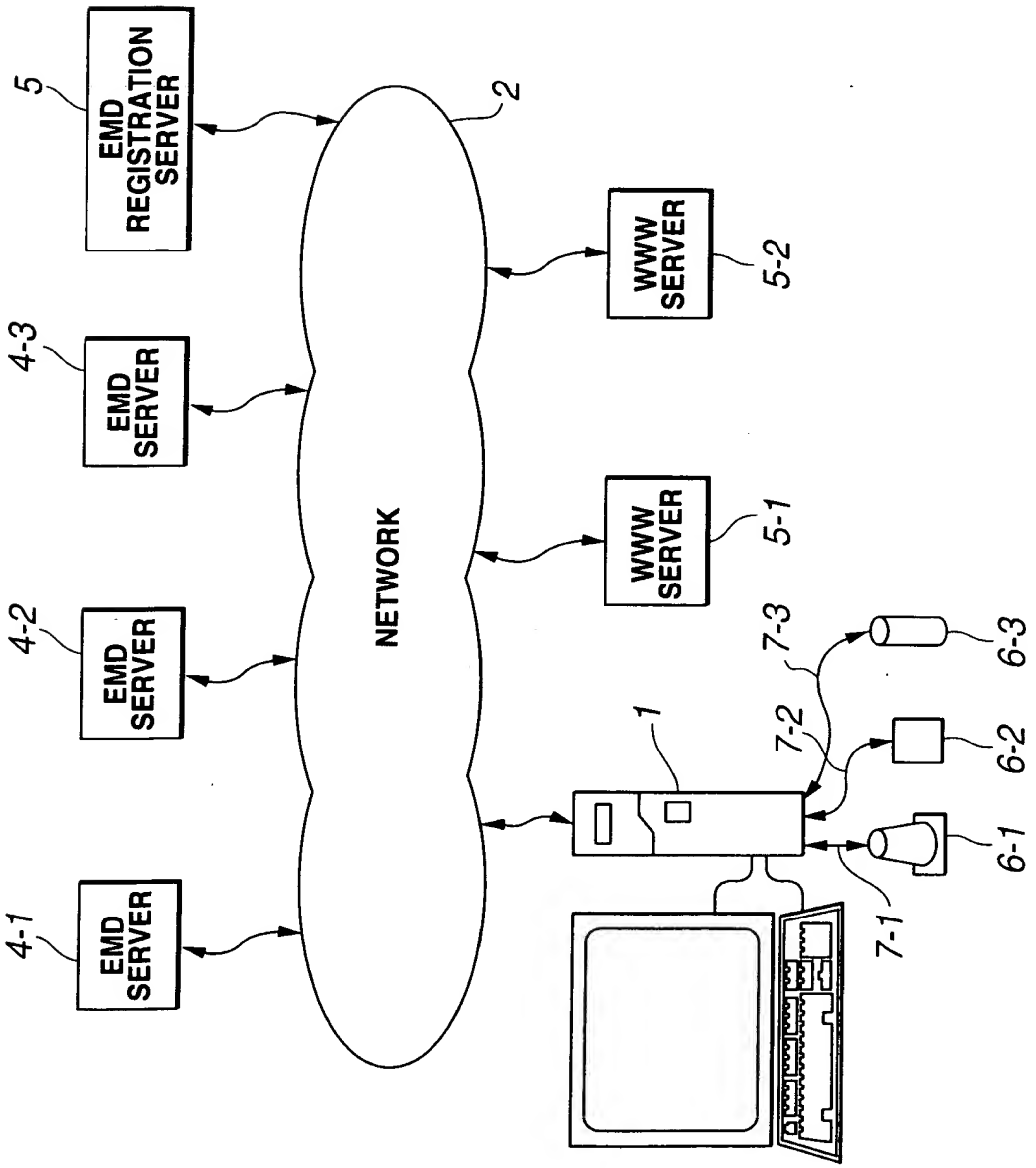

FIG.1

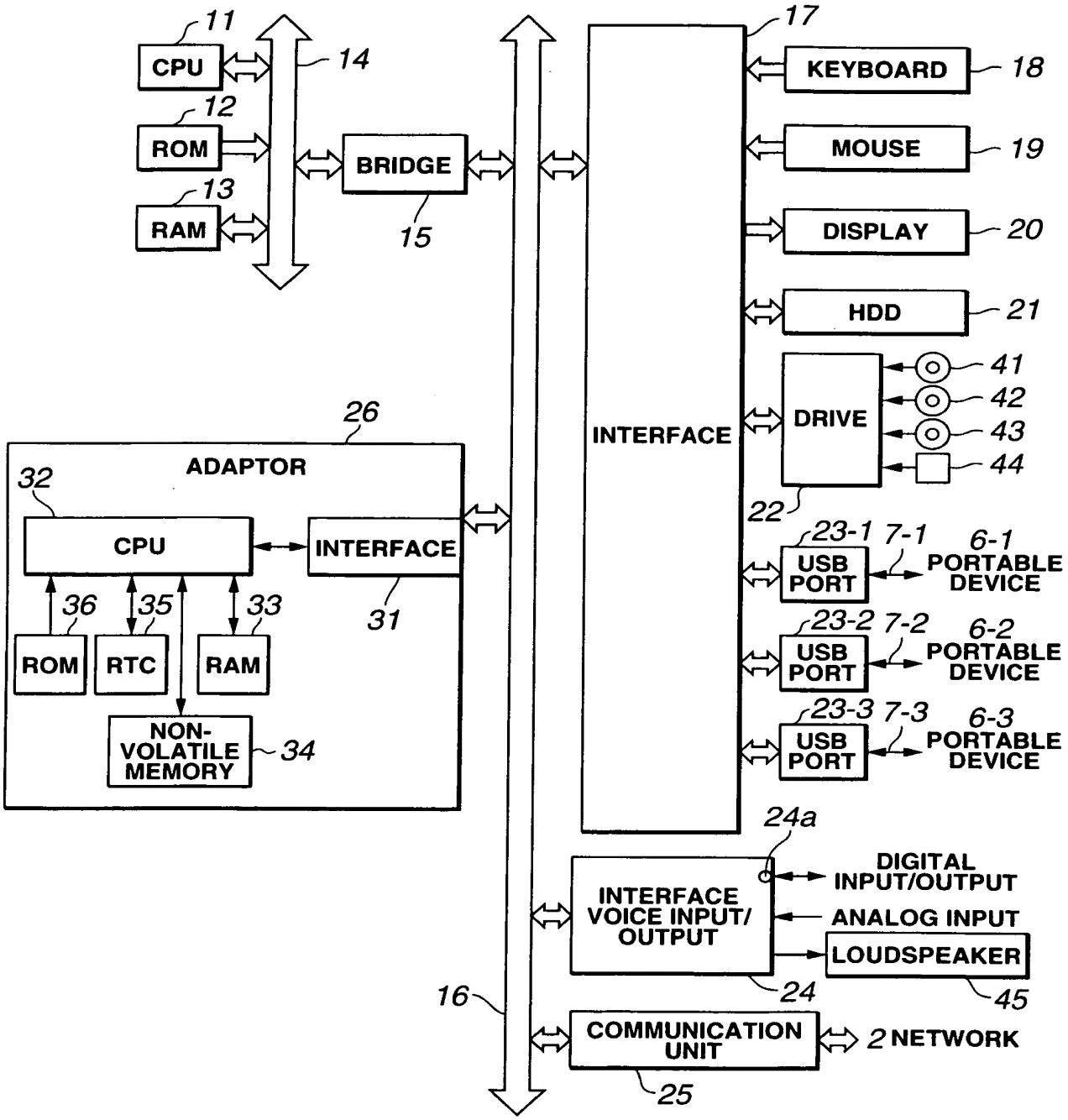
11
CPU
12
ROM
13
RAM
14
BRIDGE
15
17
INTERFACE
KEYBOARD
18
MOUSE
19
DISPLAY
20
HDD
21
DRIVE
41
42
43
44
22
23-1
USB PORT
7-1
6-1
PORTABLE DEVICE
23-2
USB PORT
7-2
6-2
PORTABLE DEVICE
23-3
USB PORT
7-3
6-3
PORTABLE DEVICE
26
ADAPTOR
32
CPU
INTERFACE
31
36
35
33
ROM
RTC
RAM
NON-VOLATILE MEMORY
34
24a
INTERFACE VOICE INPUT/ OUTPUT
DIGITAL INPUT/OUTPUT
ANALOG INPUT
LOUDSPEAKER
24
45
16
COMMUNICATION UNIT
2 NETWORK
25

FIG.2

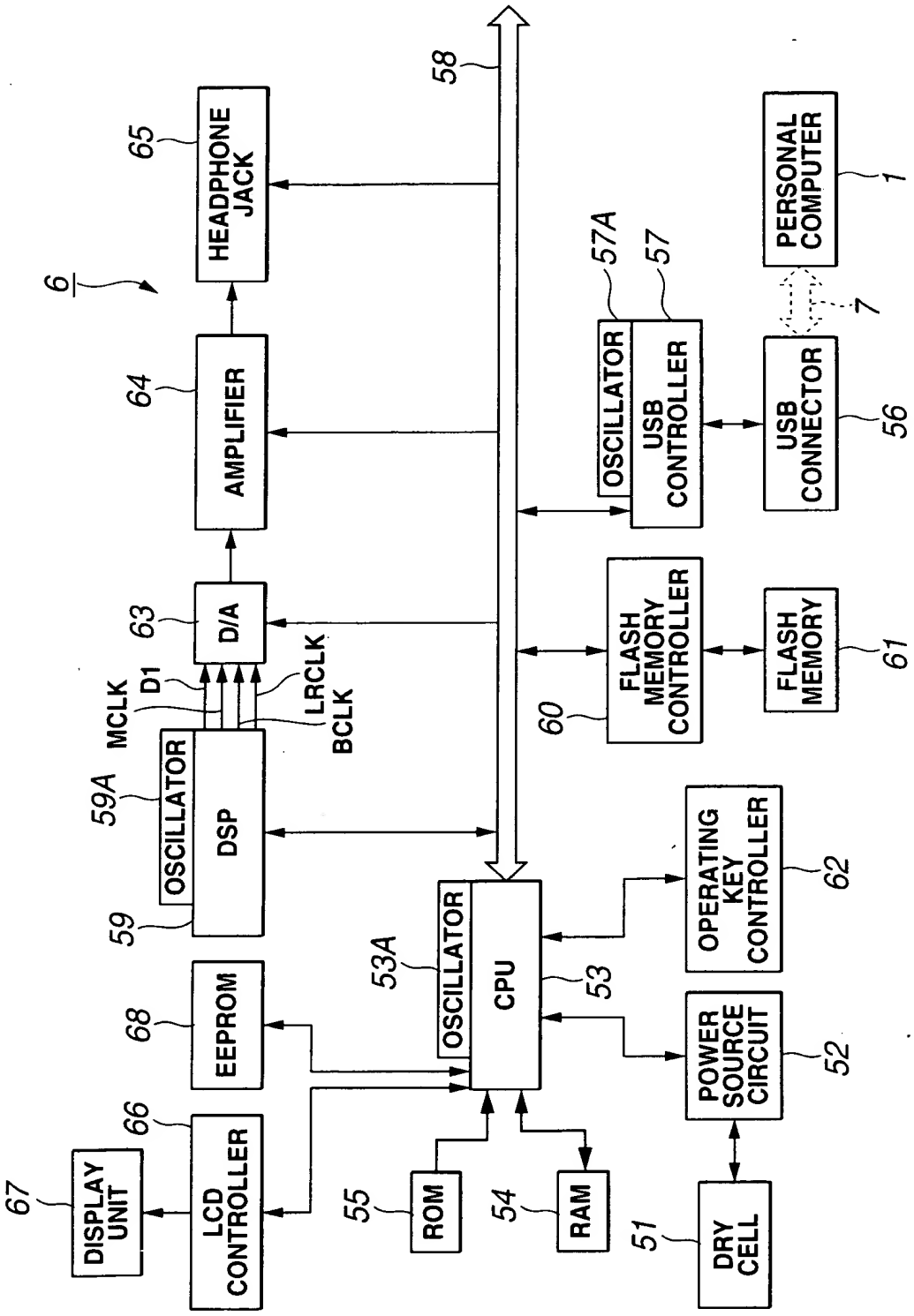
6
HEADPHONE JACK
65
AMPLIFIER
64
D/A
63
MCLK
D1
LRCLK
BCLK
OSCILLATOR
59A
DSP
59
58
PERSONAL COMPUTER
1
7
OSCILLATOR
57A
USB CONTROLLER
57
USB CONNECTOR
56
FLASH MEMORY CONTROLLER
60
FLASH MEMORY
61
OPERATING KEY CONTROLLER
62
OSCILLATOR
53A
CPU
53
POWER SOURCE CIRCUIT
52
EEPROM
68
LCD CONTROLLER
66
DISPLAY UNIT
67
ROM
55
RAM
54
DRY CELL
51

FIG.3

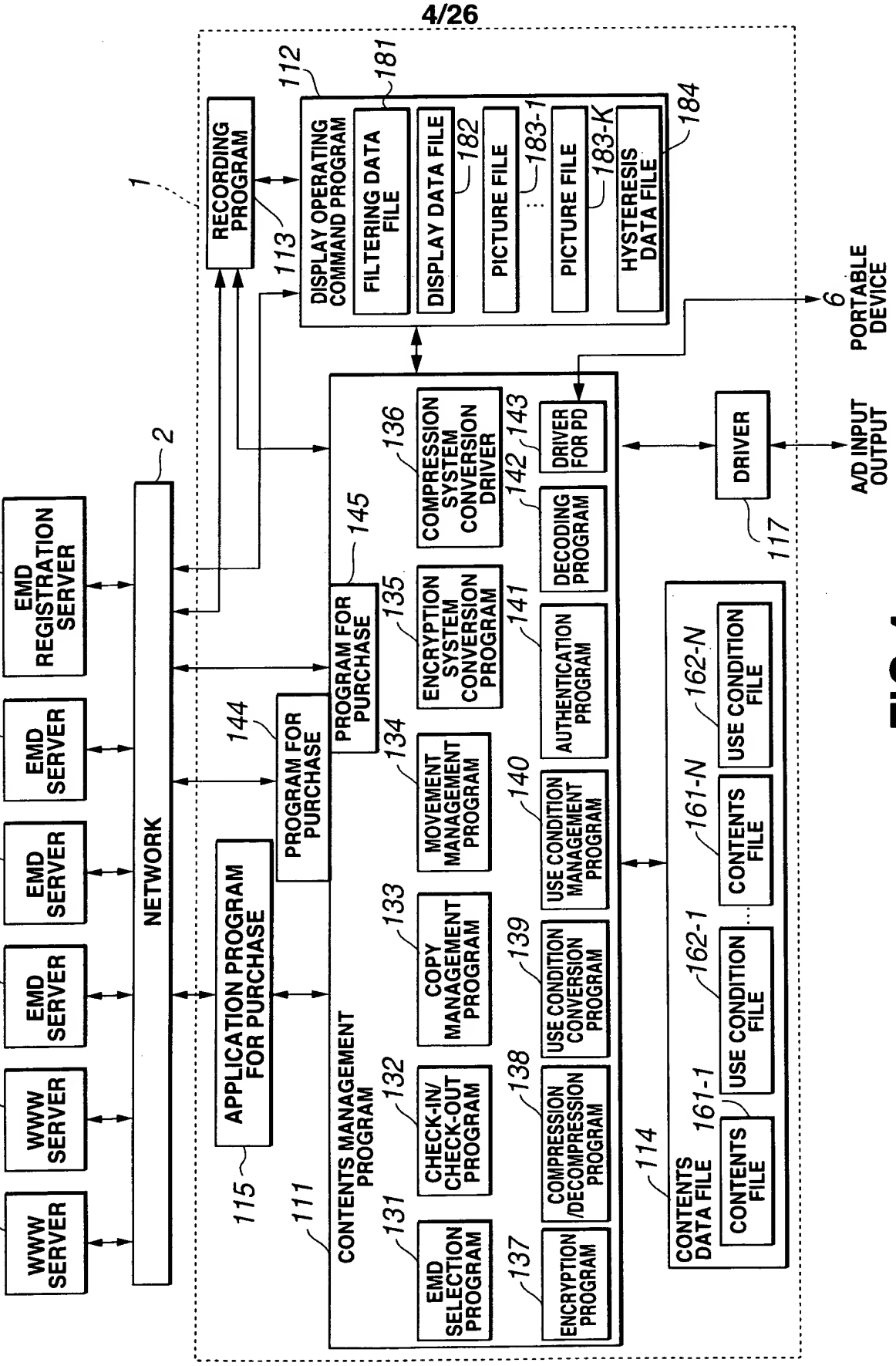
1
2
3
4-1
4-2
4-3
5-1
5-2
6
NETWORK
WWW SERVER
WWW SERVER
EMD SERVER
EMD SERVER
EMD SERVER
EMD REGISTRATION SERVER
PORTABLE DEVICE
A/D INPUT OUTPUT
RECORDING PROGRAM
DISPLAY OPERATING COMMAND PROGRAM
FILTERING DATA FILE
DISPLAY DATA FILE
PICTURE FILE
PICTURE FILE
HYSTERESIS DATA FILE
DRIVER
DRIVER FOR PD
COMPRESSION SYSTEM CONVERSION DRIVER
DECODING PROGRAM
AUTHENTICATION PROGRAM
ENCRYPTION SYSTEM CONVERSION PROGRAM
MOVEMENT MANAGEMENT PROGRAM
USE CONDITION MANAGEMENT PROGRAM
COPY MANAGEMENT PROGRAM
USE CONDITION CONVERSION PROGRAM
COMPRESSION /DECOMPRESSION PROGRAM
CHECK-IN/ CHECK-OUT PROGRAM
EMD SELECTION PROGRAM
ENCRYPTION PROGRAM
PROGRAM FOR PURCHASE
PROGRAM FOR PURCHASE
APPLICATION PROGRAM FOR PURCHASE
CONTENTS MANAGEMENT PROGRAM
CONTENTS DATA FILE
CONTENTS FILE
USE CONDITION FILE
CONTENTS FILE
USE CONDITION FILE
USE CONDITION FILE
111
112
113
114
115
117
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
161-1
161-N
162-1
162-N
181
182
183-1
183-K
184

FIG.4

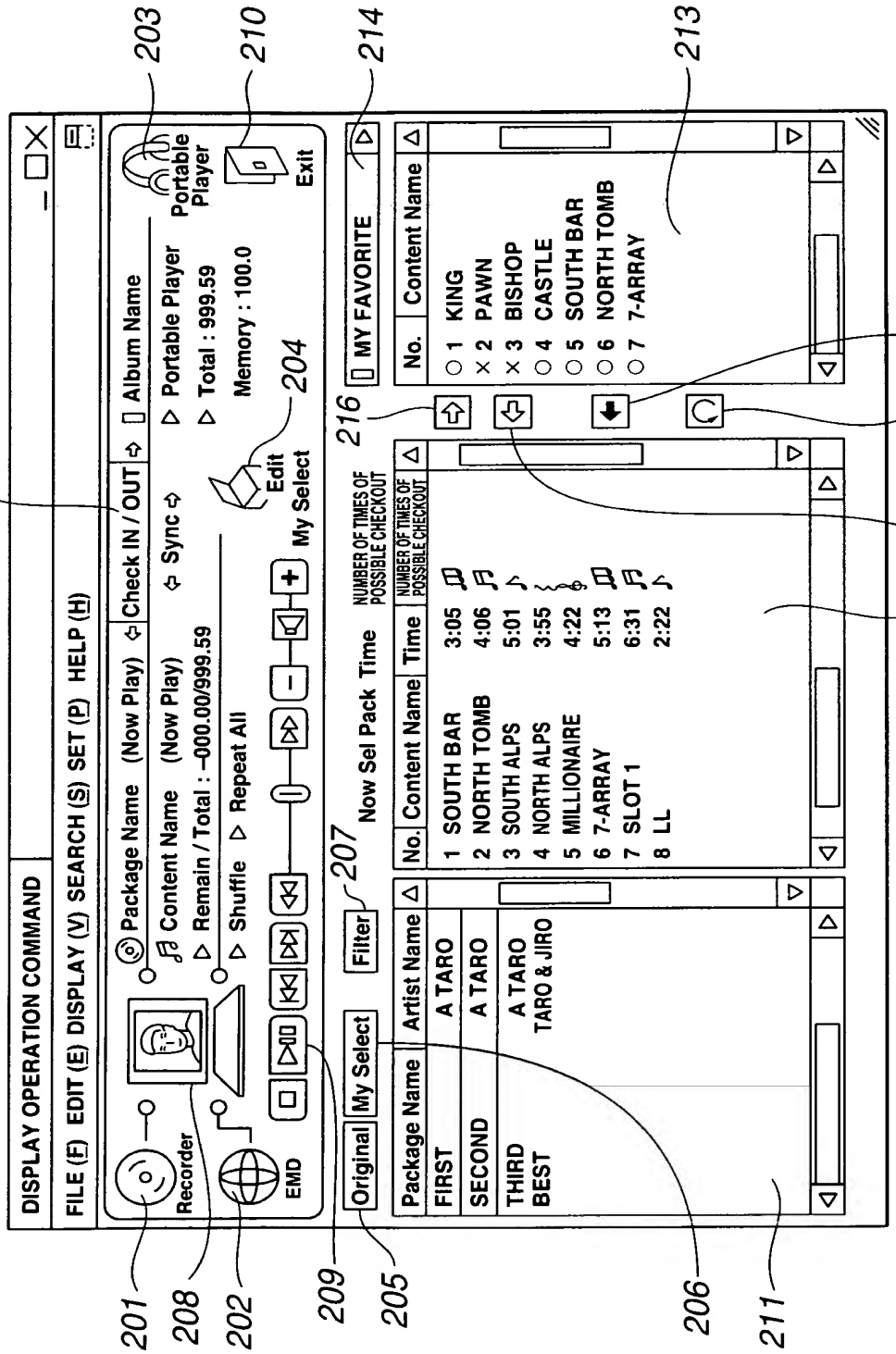
DISPLAY OPERATION COMMAND
FILE (F) EDIT (E) DISPLAY (V) SEARCH (S) SET (P) HELP (H)
Package Name (Now Play)
Check IN / OUT
Album Name
Content Name (Now Play)
Sync
Portable Player
Remain / Total : -000.00/999.59
Total : 999.59
Memory : 100.0
Shuffle
Repeat All
Edit
My Select
Recorder
EMD
Original
My Select
Filter
Now Sel Pack Time
NUMBER OF TIMES OF POSSIBLE CHECKOUT
MY FAVORITE
Portable Player
Exit
No. Content Name
1 KING
2 PAWN
3 BISHOP
4 CASTLE
5 SOUTH BAR
6 NORTH TOMB
7 7-ARRAY
No. Content Name Time
1 SOUTH BAR 3:05
2 NORTH TOMB 4:06
3 SOUTH ALPS 5:01
4 NORTH ALPS 3:55
5 MILLIONAIRE 4:22
6 7-ARRAY 5:13
7 SLOT 1 6:31
8 LL 2:22
Package Name Artist Name
FIRST A TARO
SECOND A TARO
THIRD A TARO
BEST TARO & JIRO
201
208
202
209
205
206
211
212
217
219
218
216
215
204
214
213
210
203
207

FIG.5

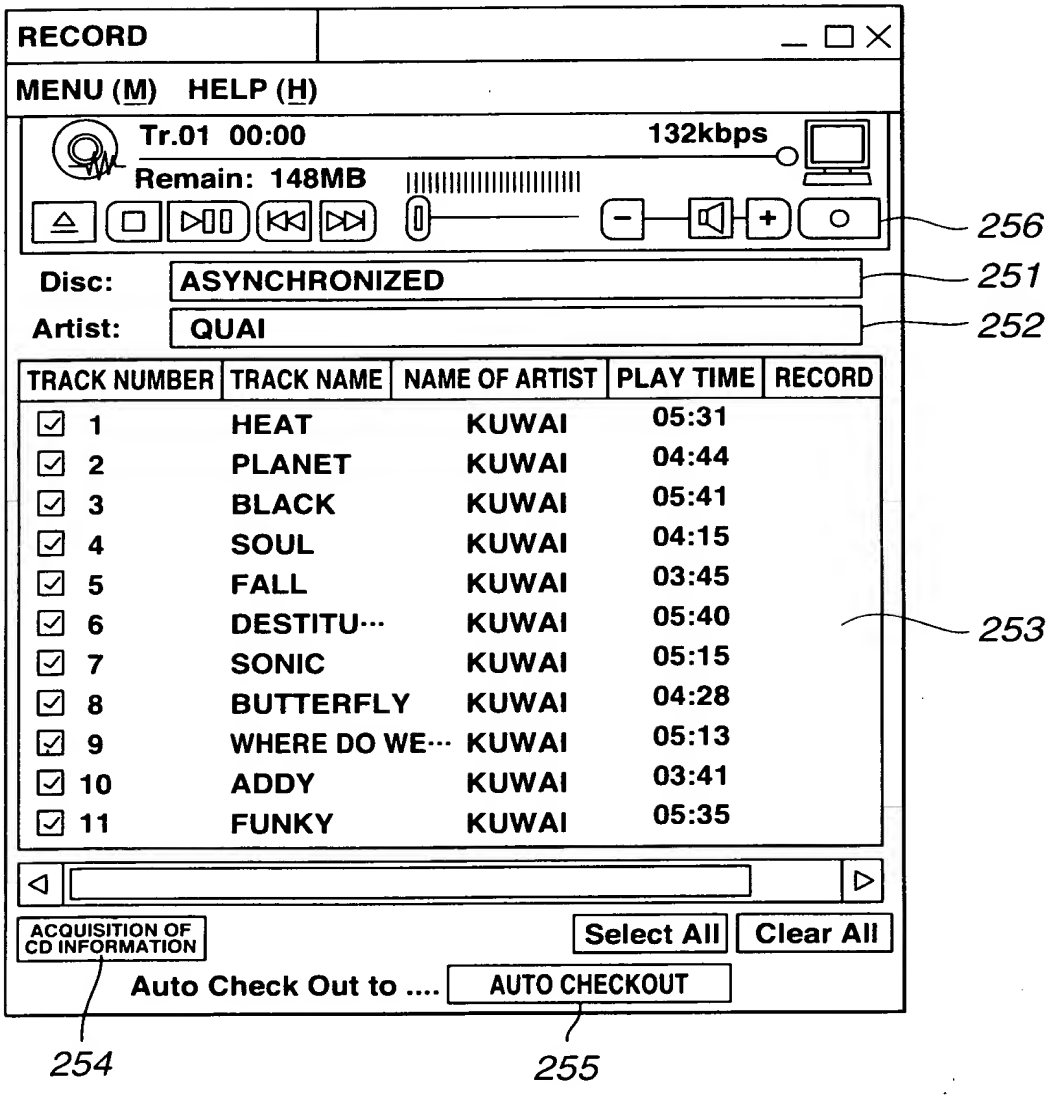
RECORD
MENU (M) HELP (H)
Tr.01 00:00
132kbps
Remain: 148MB
256
Disc: ASYNCHRONIZED
251
Artist: QUAI
252
TRACK NUMBER | TRACK NAME | NAME OF ARTIST | PLAY TIME | RECORD
1 HEAT KUWAI 05:31
2 PLANET KUWAI 04:44
3 BLACK KUWAI 05:41
4 SOUL KUWAI 04:15
5 FALL KUWAI 03:45
6 DESTITU··· KUWAI 05:40
7 SONIC KUWAI 05:15
8 BUTTERFLY KUWAI 04:28
9 WHERE DO WE··· KUWAI 05:13
10 ADDY KUWAI 03:41
11 FUNKY KUWAI 05:35
253
ACQUISITION OF CD INFORMATION
Select All
Clear All
Auto Check Out to ....
AUTO CHECKOUT
254
255

FIG.6

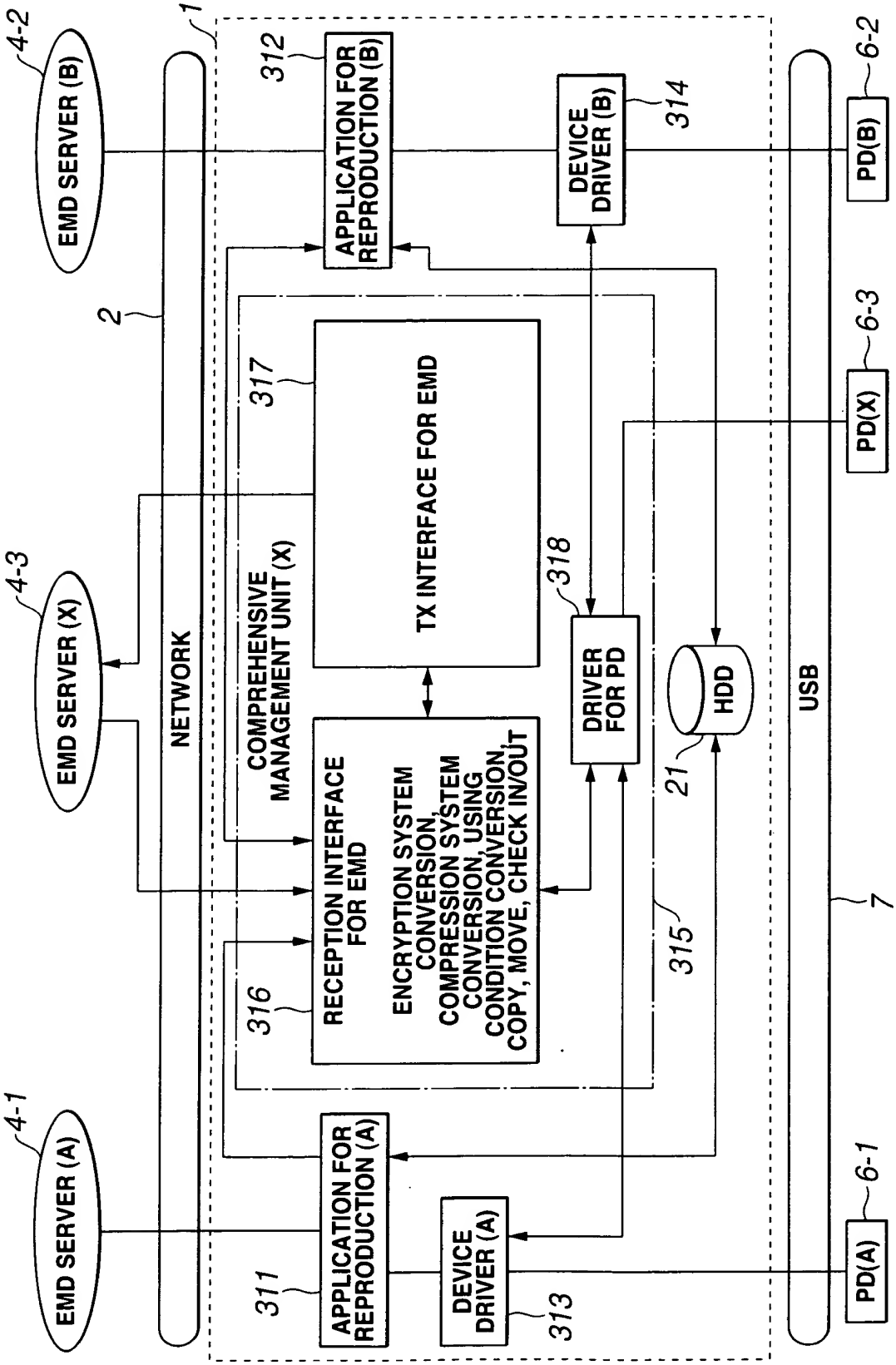
EMD SERVER (B)
EMD SERVER (X)
EMD SERVER (A)
NETWORK
APPLICATION FOR REPRODUCTION (B)
APPLICATION FOR REPRODUCTION (A)
DEVICE DRIVER (B)
DEVICE DRIVER (A)
COMPREHENSIVE MANAGEMENT UNIT (X)
TX INTERFACE FOR EMD
RECEPTION INTERFACE FOR EMD
ENCRYPTION SYSTEM CONVERSION, COMPRESSION SYSTEM CONVERSION, USING CONDITION CONVERSION, COPY, MOVE, CHECK IN/OUT
DRIVER FOR PD
HDD
USB
PD(B)
PD(X)
PD(A)
1
2
4-1
4-2
4-3
6-1
6-2
6-3
7
21
311
312
313
314
315
316
317
318

FIG.7

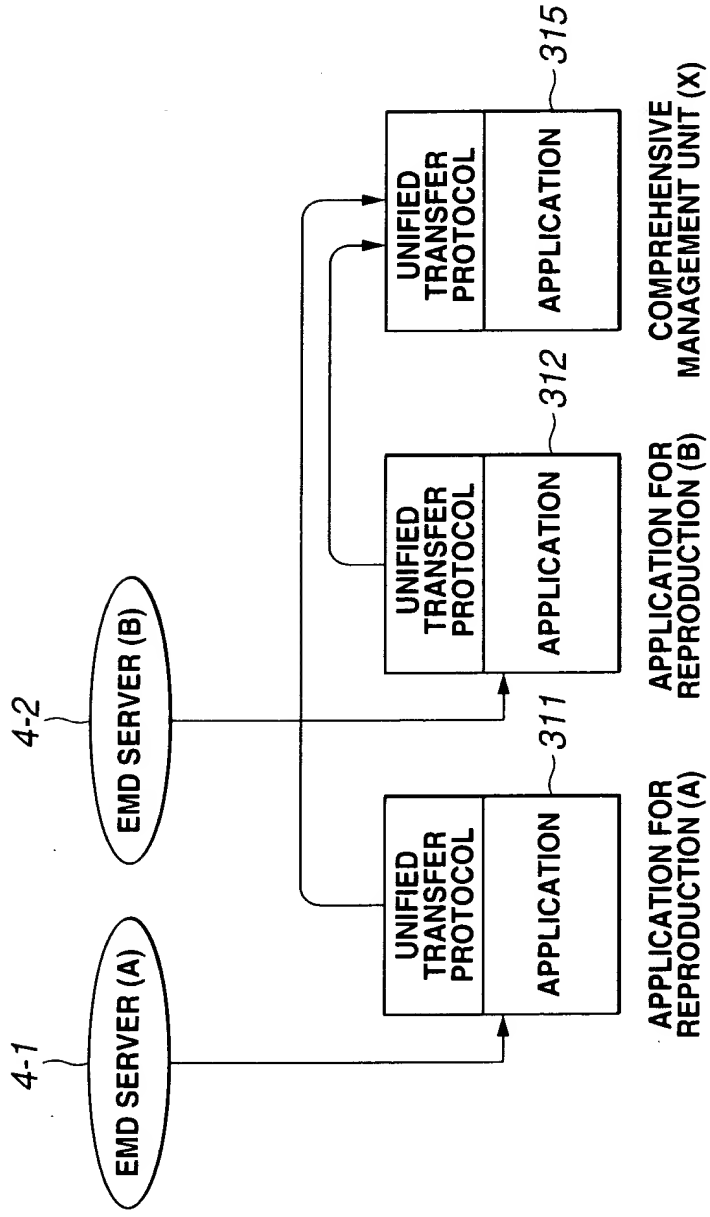
4-1
EMD SERVER (A)
4-2
EMD SERVER (B)
UNIFIED TRANSFER PROTOCOL
APPLICATION
311
APPLICATION FOR REPRODUCTION (A)
UNIFIED TRANSFER PROTOCOL
APPLICATION
312
APPLICATION FOR REPRODUCTION (B)
UNIFIED TRANSFER PROTOCOL
APPLICATION
315
COMPREHENSIVE MANAGEMENT UNIT (X)

FIG.8

FIG.9A

POLICY	VALUE
from	99/10/25
to	99/11/24
pay/play	yes/10yen

FIG.9B

CONTENTS
USING CONDITION INFORMATION

INDEX FILE	331
AUTOMATON FILE	332
PARAMETER FILE	333
HYSTERESIS FILE	334

FIG.10

Automaton	341
MAC_{K_C} (Automaton)	342
$Sig_{K_E}^{-1}$ (Automaton)	343
Cert (K_E^1)	344

FIG.11

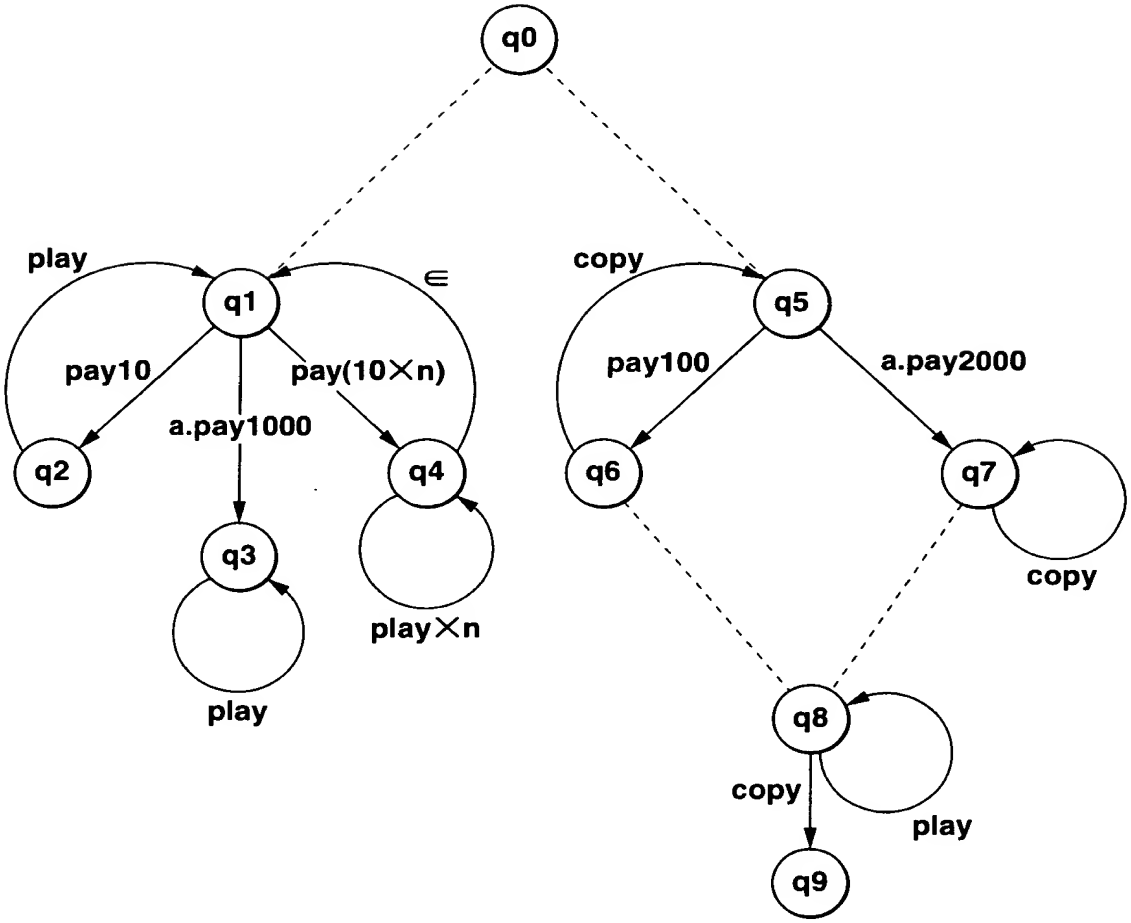
q0
play
q1
∈
pay10
pay(10×n)
a.pay1000
q2
q3
q4
play
play×n
copy
q5
pay100
a.pay2000
q6
q7
copy
q8
copy
play
q9

FIG.12

$\langle q_1, pay10, q_2 \rangle$
$\langle q_1, a.pay1000, q_3 \rangle$
$\langle q_1, pay(10 \times n), q_4 \rangle$
$\langle q_2, play, q_1 \rangle$
$\langle q_3, play, q_3 \rangle$
$\langle q_4, play \times n, q_4 \rangle$
$\langle q_4, \varepsilon, q_1 \rangle$
$\langle q_5, pay100, q_6 \rangle$
$\langle q_5, a.pay2000, q_7 \rangle$
$\langle q_6, copy, q_5 \rangle$
$\langle q_7, copy, q_7 \rangle$
$\langle q_8, play, q_8 \rangle$
$\langle q_8, copy, q_9 \rangle$

FIG.13

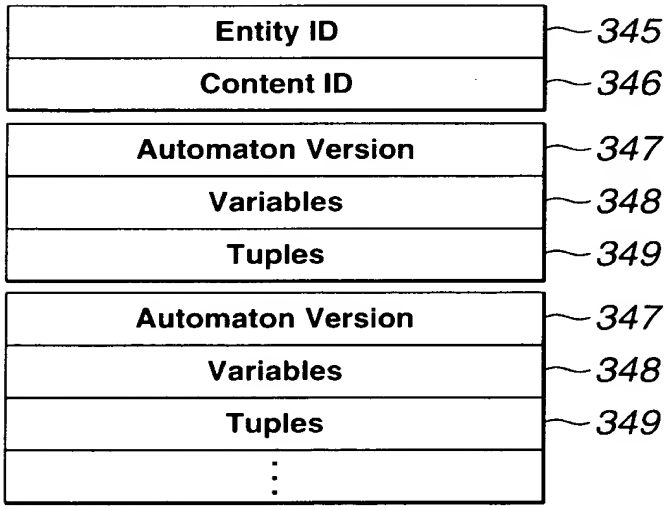

FIG.14

```
<!ENTITY% event" (
        play                    1
        copy                    1
        pay-for-play            1
        pay-for-copy            1
        pay-for-album-play      1
        pay-for-album-copy      1
        from                    1
        to                      1
        null                    1
)">
<!ENTITY% command" (
        drop                    1
        dup                     1
        swap                    1
        add                     1
        subtract                1
        multiply                1
        divide                  1
        remainder               1
        upper                   1
        lower                   1
        equal                   1
        less                    1
        greater                 1
        less-equal              1
        greater-equal           1
        and                     1
        or                      1
        not                     1
        bit-and                 1
        bit-or                  1
        bit-xor                 1
        bit-not                 1
)">
```

FIG.15

Content playable from 1999/9/1

```
<automaton>

   <!—This usage rule system has one Right Unit.
   Initial state is q1- ->
    <Initial-right-unit state="q1"/>

   <node state = "q1">
     <!—If after 1999/9/1, transfer to q2- ->
     <rule event="from" next-state="q2">
       <arguments>
         <integer value="time:19990901"/>
       </arguments>
     </rule>
   </node>

   <node state = "q2">
     <!- - playable - ->
     <rule event="play" next-state="q2"/>
   </node>

</automaton>
```

FIG.16

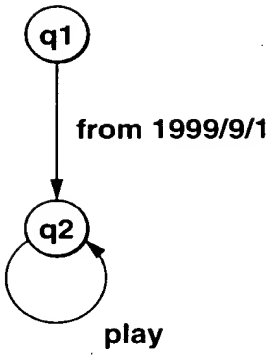

FIG.17

Content playable until 1999/10/31

```
<automaton>

   <!- - This Usage Rule System has one Right Unit.
   Initial state is q2 - ->
    <Initial-right-unit state="q2"/>

   <node state = "q2">
     <!—If after 1999/10/31, transfer to end - ->
     <rule event="to" next-state="end">
       <arguments>
         <integer value="time:19991031"/>
       </arguments>
     </rule>

     <!- - playable - ->
     <rule event="play" next-state="q2">
     </rule>
   </node>

   <!—Unusable state - ->
   <node state = "end"/>

</automaton>
```

FIG.18

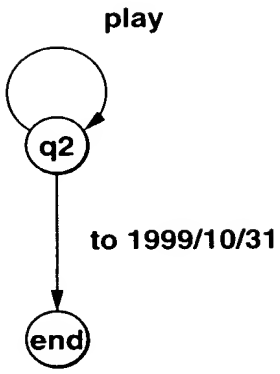

FIG.19

Content playable 16 times from 1999/9/1 to 1999/10/31

```
<automaton>

  <!--Define counter variables for playable numbers. Initial value is 16 -->
  <define-variable name="count" initial-value="16" />

  <!-- This Usage Rule System has one Right Unit. Initial state is q1 -->
  <initial-right-unit state="q1" />

  <node state="q1">
    <!--From 1999/9/1 transfer to q2 -->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time:19990901" />
      </arguments>
    </rule>
  </node>

  <node state="q2">
    <!--From 1999/10/31, transfer to end -->
    <rule event="to" next-state="end">
      <arguments>
        <integer value="time:19991031" />
      </arguments>
    </rule>

    <rule event="play" next-state="q2">
      <!--Playable only for "count" numbers -->
      <arguments>
        <variable name="count" />
        <command name="load" />
      </arguments>
      <!--If this rule is selected, the "count" number decrements by one-->
      <action>
        <variable name="count" />
        <command name="load" />
        <integer value="1" />
        <command name="subtract" />
        <variable name="count" />
        <command name="store" />
      </action>
    </rule>
  </node>

  <!--Unusable state-->
  <node state="end" />

</automaton>
```

FIG.20

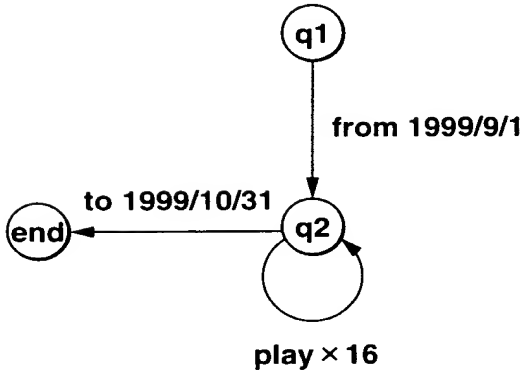

FIG.21

Content playable less than and/or equal to 16 times

```
<automaton>

  <!--Define valuable counter for playable numbers. Initial value is 16 -->
  <define-variable name="count" initial-value="16" />

  <!-- Usage Rule System has one Right Unit. Initial state is q2 -->
  <initial-right-unit state="q1" />

  <node state="q2">
    <rule event="play" next-state="q2">
      <!--"Count" number of times playable -->
      <arguments>
        <variable name="count" />
        <command name="load" />
      </arguments>
      <!--If this rule is selected. "count" number decrements by one-->
      <action>
        <variable name="count" />
        <command name="load" />
        <integer value="1" />
        <command name="subtract" />
        <variable name="count" />
        <command name="store" />
      </action>
    </rule>
  </node>

</automaton>
```

FIG.22

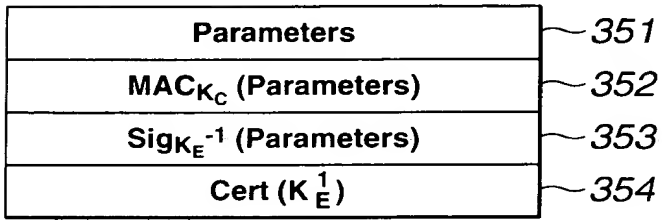

FIG.23

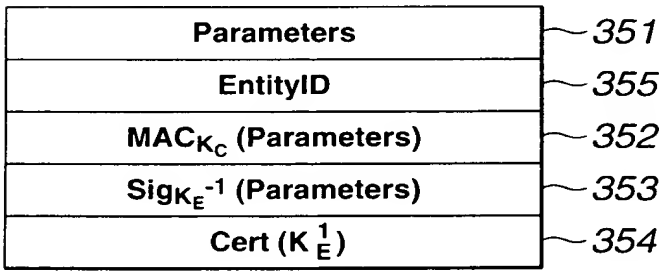

FIG.24

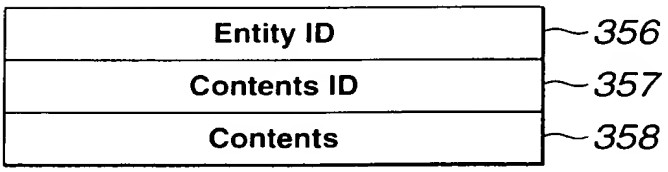

FIG.25

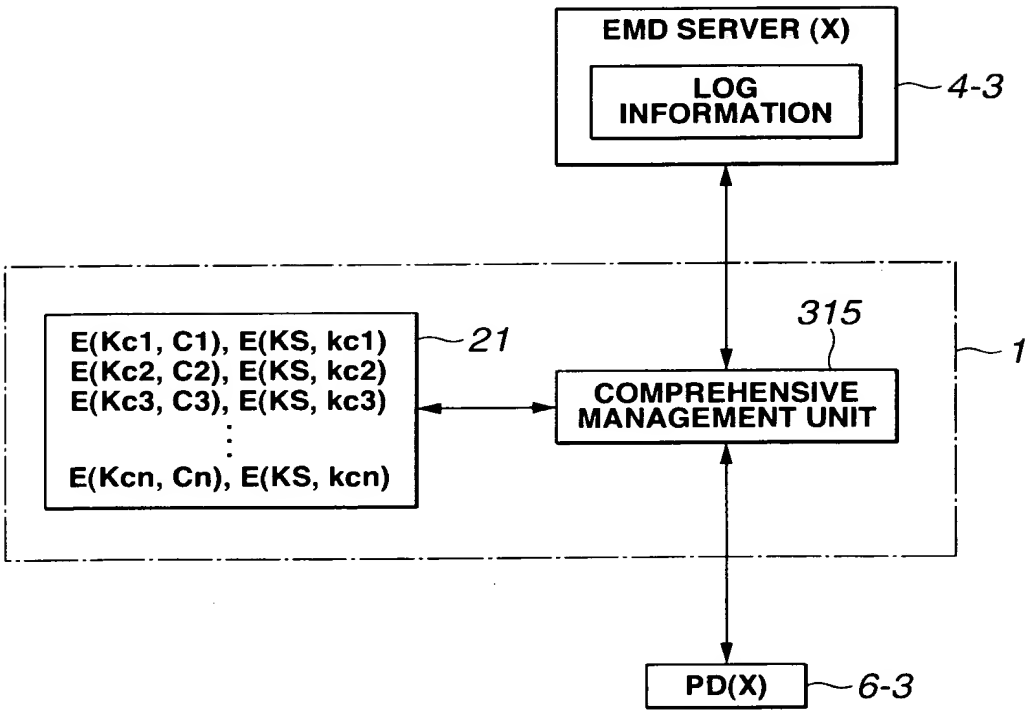
EMD SERVER (X)
LOG INFORMATION
4-3
315
1
E(Kc1, C1), E(KS, kc1)
E(Kc2, C2), E(KS, kc2)
E(Kc3, C3), E(KS, kc3)
E(Kcn, Cn), E(KS, kcn)
21
COMPREHENSIVE MANAGEMENT UNIT
PD(X)
6-3

FIG.26

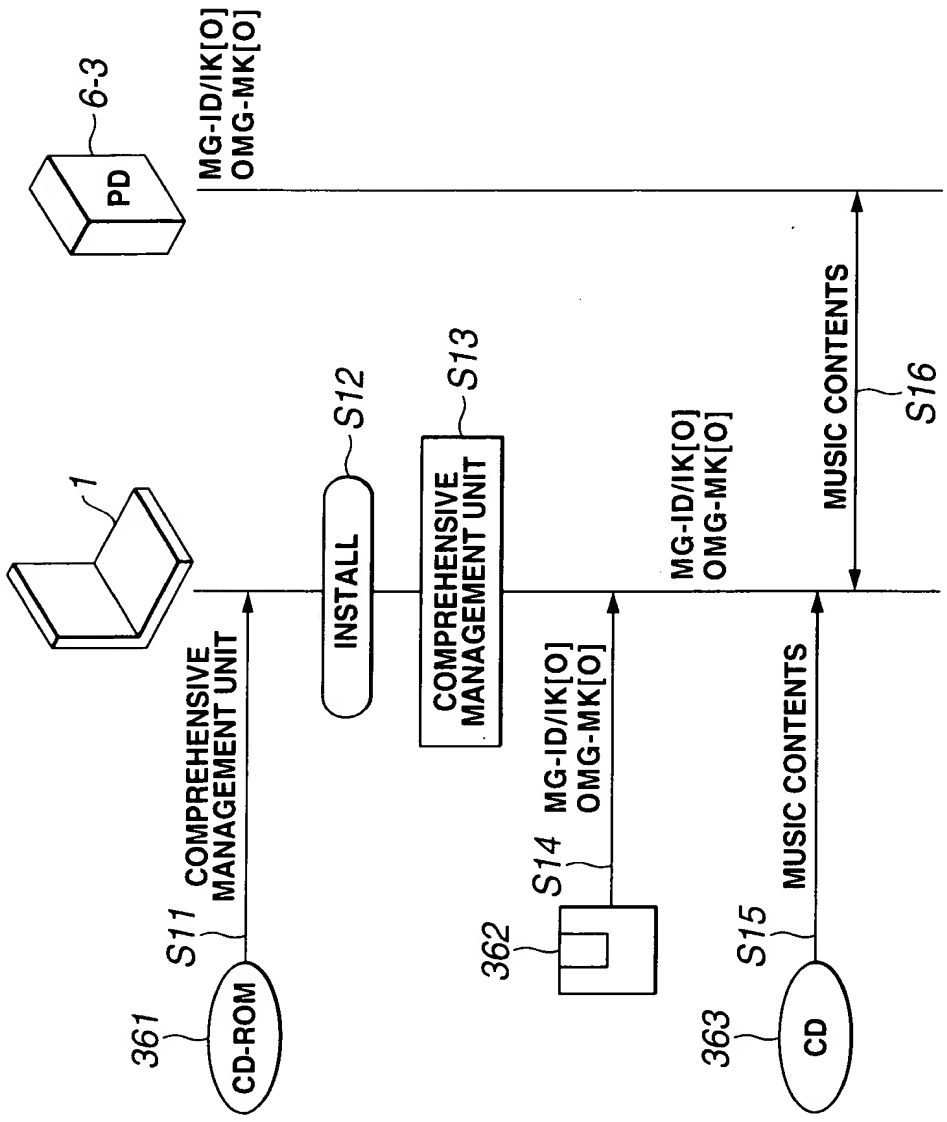
6-3
PD
MG-ID/IK[O]
OMG-MK[O]
1
S12
INSTALL
S13
COMPREHENSIVE
MANAGEMENT UNIT
MG-ID/IK[O]
OMG-MK[O]
MUSIC CONTENTS
S16
COMPREHENSIVE
MANAGEMENT UNIT
S11
MG-ID/IK[O]
OMG-MK[O]
S14
MUSIC CONTENTS
S15
361
CD-ROM
362
363
CD

FIG.27

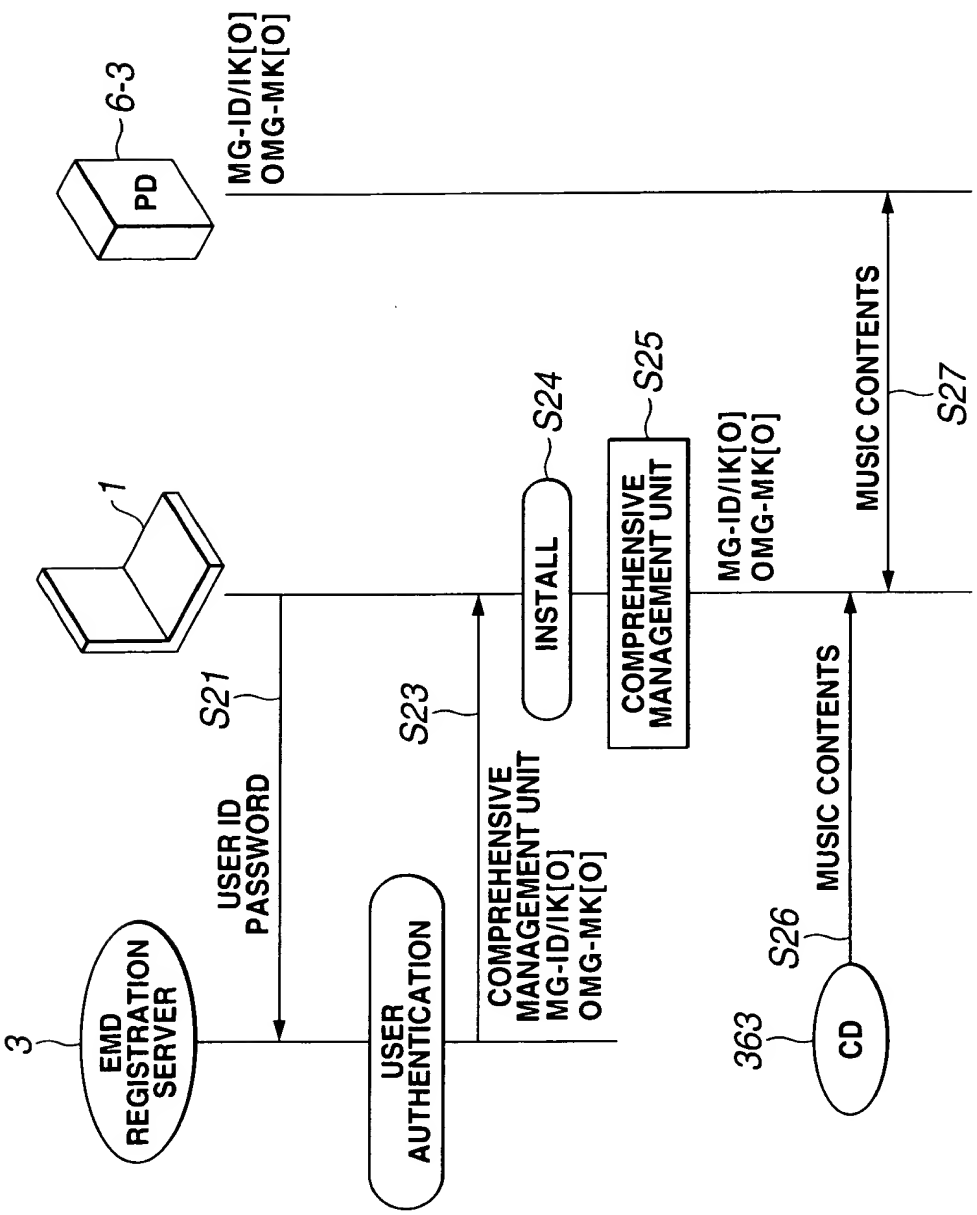
3
EMD REGISTRATION SERVER
USER ID PASSWORD
S21
USER AUTHENTICATION
S23
COMPREHENSIVE MANAGEMENT UNIT MG-ID/IK[O] OMG-MK[O]
1
INSTALL
S24
COMPREHENSIVE MANAGEMENT UNIT
S25
MG-ID/IK[O] OMG-MK[O]
6-3
PD
MG-ID/IK[O] OMG-MK[O]
MUSIC CONTENTS
S27
363
CD
S26
MUSIC CONTENTS

FIG.28

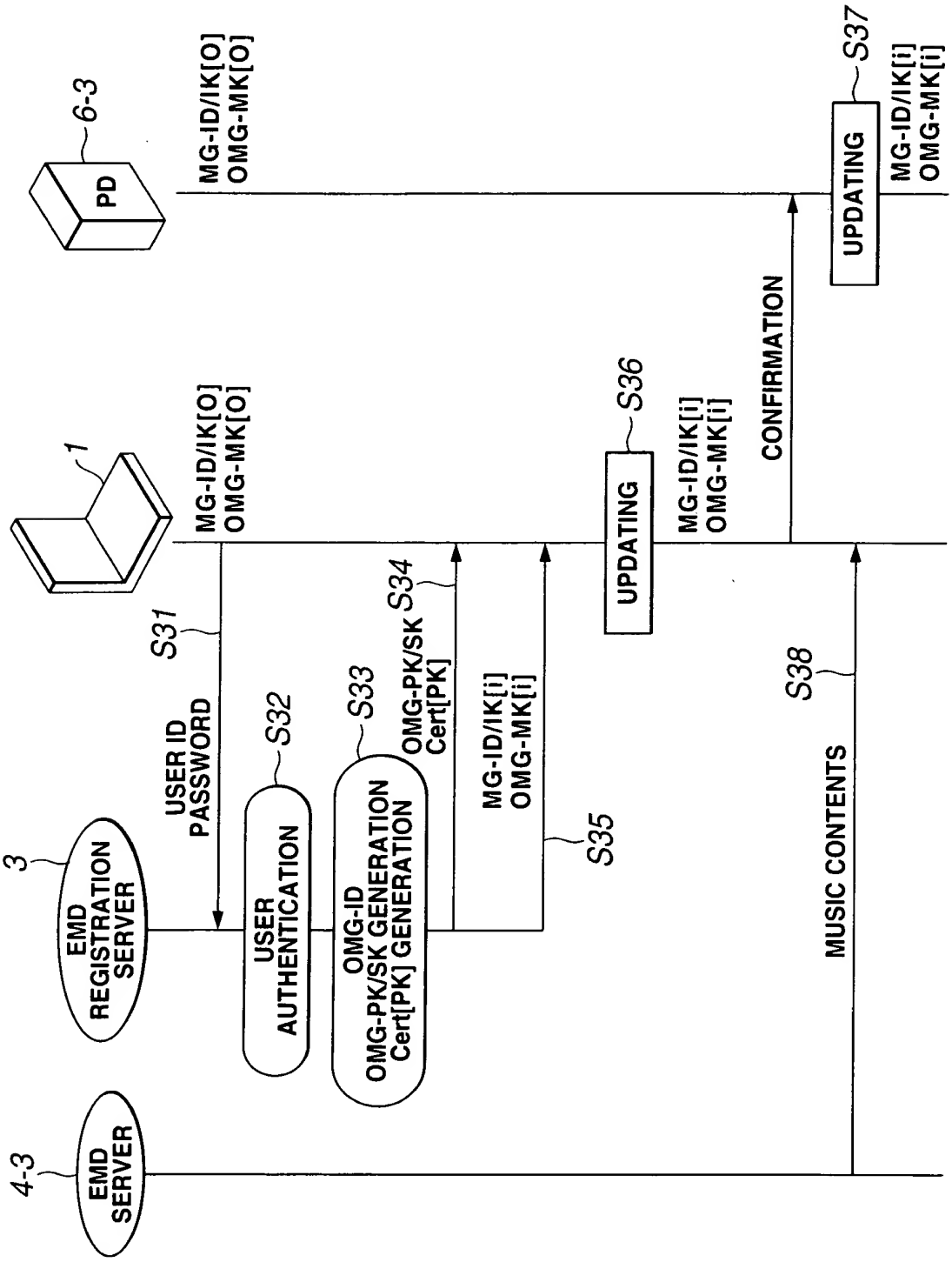
6-3
PD
MG-ID/IK[O]
OMG-MK[O]
S37
UPDATING
MG-ID/IK[i]
OMG-MK[i]
1
MG-ID/IK[O]
OMG-MK[O]
S36
UPDATING
MG-ID/IK[i]
OMG-MK[i]
CONFIRMATION
S31
USER ID
PASSWORD
S32
S33
OMG-PK/SK
Cert[PK]
S34
MG-ID/IK[i]
OMG-MK[i]
S35
S38
MUSIC CONTENTS
3
EMD
REGISTRATION
SERVER
USER
AUTHENTICATION
OMG-ID
OMG-PK/SK GENERATION
Cert[PK] GENERATION
4-3
EMD
SERVER

FIG.29

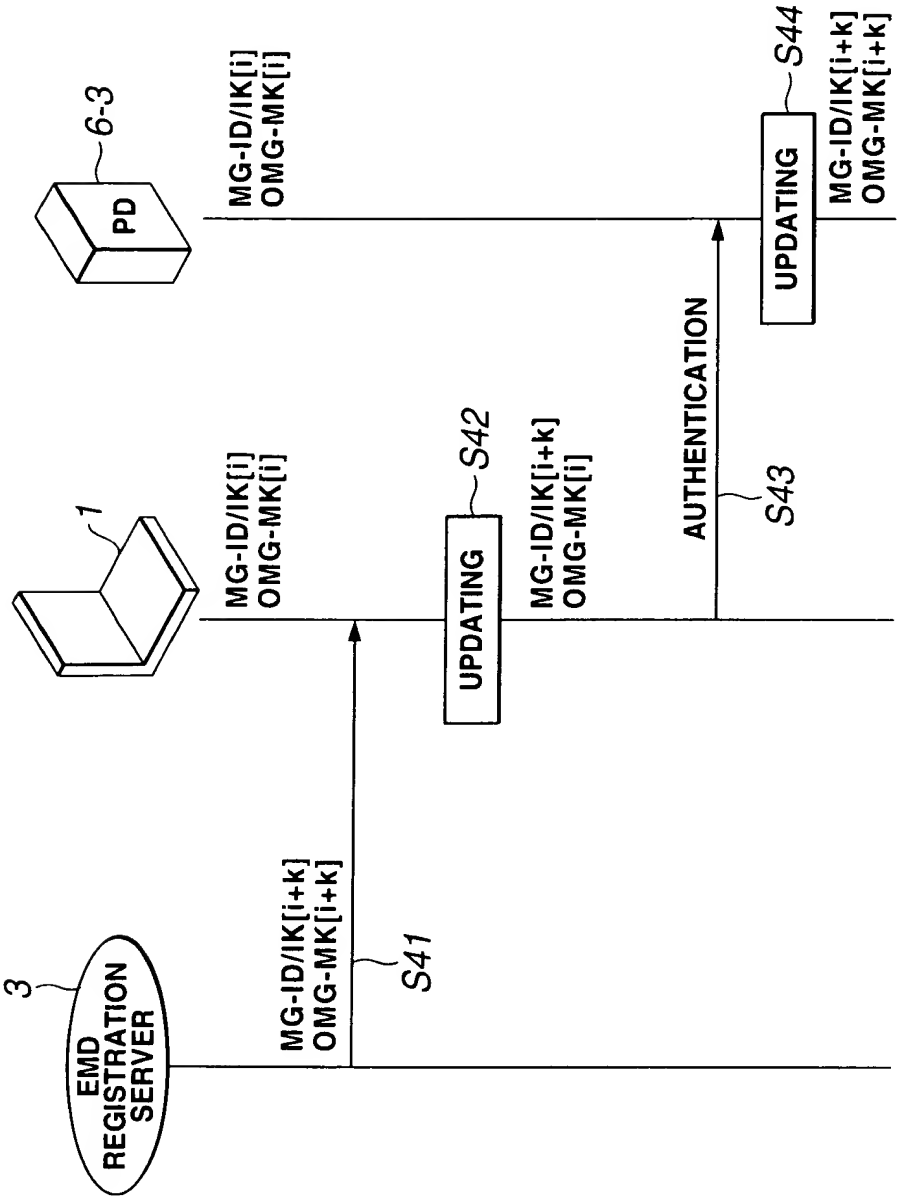
3
EMD REGISTRATION SERVER
MG-ID/IK[i+k]
OMG-MK[i+k]
S41
1
MG-ID/IK[i]
OMG-MK[i]
UPDATING
S42
MG-ID/IK[i+k]
OMG-MK[i]
AUTHENTICATION
S43
6-3
PD
MG-ID/IK[i]
OMG-MK[i]
UPDATING
S44
MG-ID/IK[i+k]
OMG-MK[i+k]

FIG.30

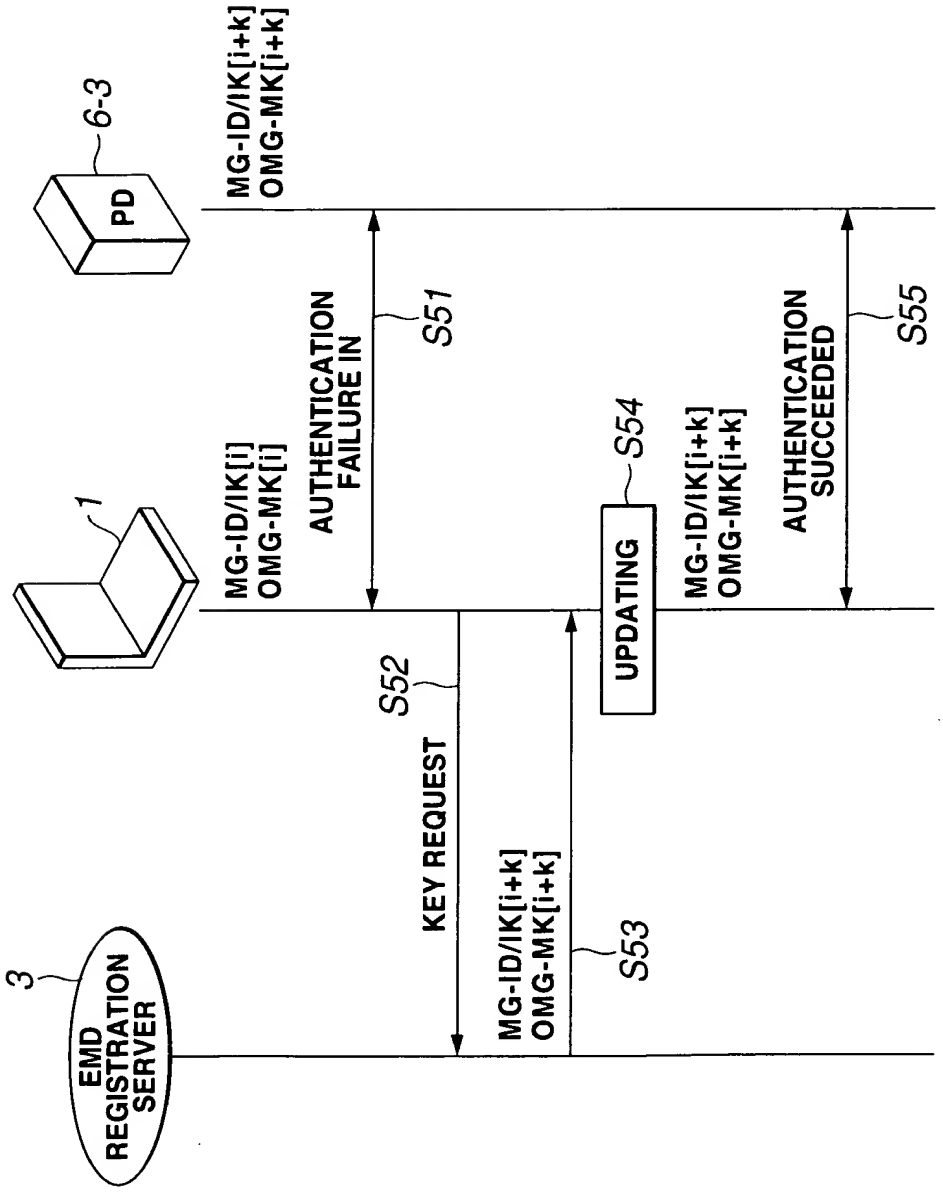
3
EMD REGISTRATION SERVER
1
6-3
PD
MG-ID/IK[i]
OMG-MK[i]
MG-ID/IK[i+k]
OMG-MK[i+k]
AUTHENTICATION FAILURE IN
S51
KEY REQUEST
S52
MG-ID/IK[i+k]
OMG-MK[i+k]
S53
UPDATING
S54
MG-ID/IK[i+k]
OMG-MK[i+k]
AUTHENTICATION SUCCEEDED
S55

FIG.31